Exploration of Blockchain for Edifying Safety and security in IoT Based Diamond International Trade

Rincy Merlin Mathew, R. Suguna, M. Shyamala Devi

Abstract: ***Recently, Internet of Things is evolving as a absolute full-fledged expertise in the field of technology that are used in all the Smart applications and it stands itself in the upcoming invention of world wide web. As like the World Wide Web, the blooming technology is the Blockchain where all the single nodes in the blockchain hold its own database as distributed ledger. The presence of the ledger enlighten the safety and unambiguous data. This blockchain technology continuously executes the code for smart contracts and consensus thereby prohibiting the access and the entry of the illegitimate clients. The unauthorized users are also not allowed to process any blunder transaction by overcrossing the smart contract code. Therefore there is a possibility of the block chain to integrate with the Internet of Things to overwhelm the performance of any real time application. By considering all this aspects, this paper discusses the preliminaries of the blockchain technology. We also attempt to propose an architectural design namely IoT Blockchain Based Diamond International Trade that provides high security and data performance. The Private Blockchain network namely Ethereum blockchain is used for implementation and the results are also discussed.***

Index Terms: Blockchain, IoT, Ledger, Smart contract, Consensus

I. INTRODUCTION

By succeeding the technology, the network transformation occurs due to the need of storage and data access capability. The desktop systems were allowed to communicate between other desktop to form a network. This further develops to form a local area network. Further, many desktop were connected under a single server to form client server network. This scenario is developed to form a centralized area network, distributed area network, Decentralized network as shown in the Fig. 1, Fig. 2 and Fig. 3.

Any real time business networks can utilize the application of blockchain technology [1]. Any individual can join the network and they can participate in processing the transaction in the block chain network. In such case the transaction executed by any individual is transparent to all the users under that blockchain. It is named as public blockchain. If the users entering the blockchain network is the authorized users then the network is private blockchain network. The transactions that are executed by all the individuals are validated and are stored in the distributed ledger [2] and it's updated to all the individuals enrolled in the blockchain.

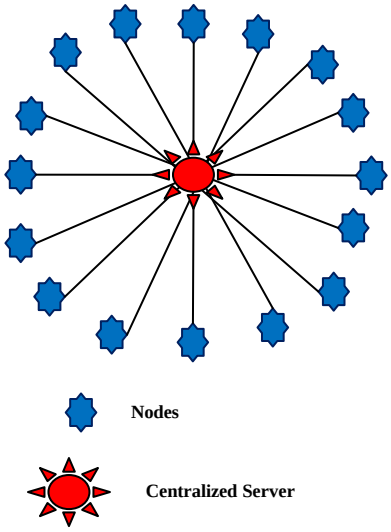

Fig. 1. Centralized System Architecture

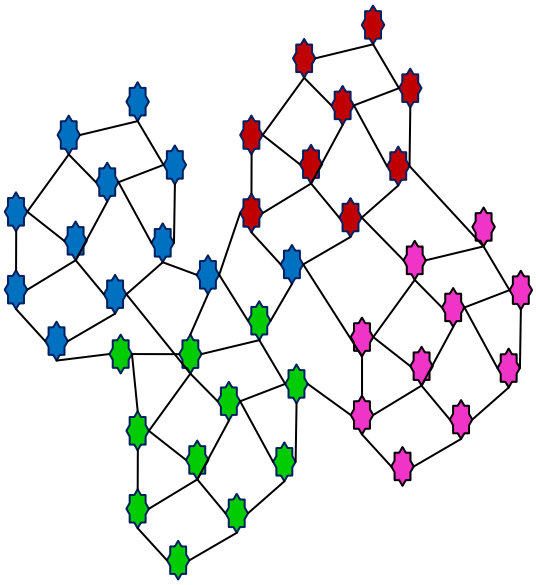

Fig. 2. Distributed System Architecture

Revised Manuscript Received on June 13, 2019

Rincy Merlin Mathew, Lecturer, Department of Computer Science, College of Science and Arts, Khamis Mushayt, King Khalid university, Abha, Asir, Saudi Arabia.

R. Suguna, Professor, Computer Science and Engineering, Vel Tech Rangarajan Dr. Sagunthala R&D Institute of Science and Technology, Avadi, Chennai, TamilNadu, India.

M. Shyamala Devi, Associate Professor, Computer Science and Engineering, Vel Tech Rangarajan Dr. Sagunthala R&D Institute of Science and Technology, Avadi, Chennai, TamilNadu, India.

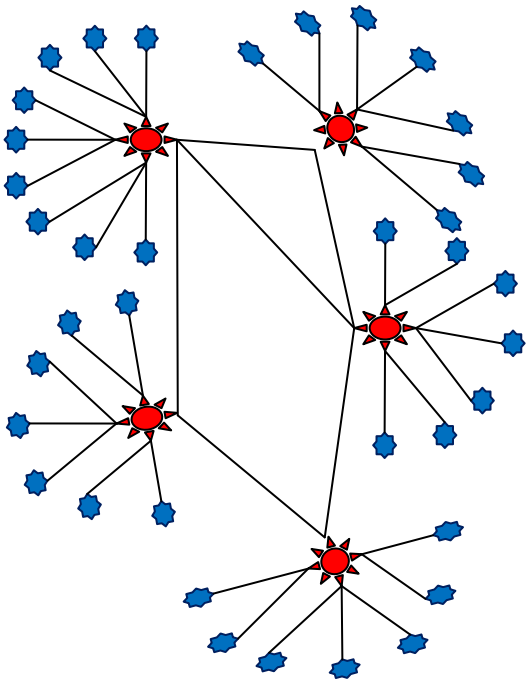

Fig. 3. DeCentralized System Architecture

II. PRELIMINARIES

A. Block Chain

Blockchain datastructure [3] consists of the following components and is shown in Fig. 4.

- ✓ Previous Block Header
- ✓ Timestamp
- ✓ Nonce
- ✓ Merkle Root Hash

The unauthorized users are not allowed to enter in the blockchain as it executes the smart contract [4] and consensus. Only if the entire individual agrees to a single then it is updated in the ledger implementing the consensus property.

.

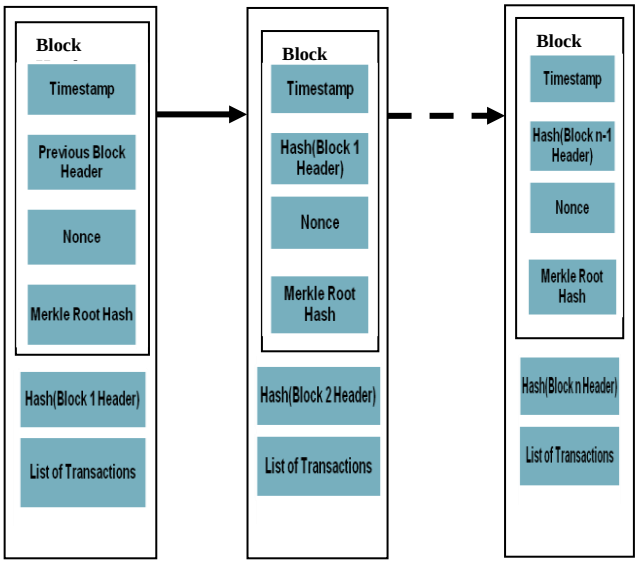

Fig. 4. Blockchain Technology

B. Smart Contracts

Manual processes that are used for making the legal contracts [5] can be automated by the execution of software code which is automatically executed by the occurrence of some actions. This set of software instruction is called as smart contracts [6]. The smart contract [7] is a module of a blockchain-based system that can automatically inflict stakeholder-agreed rules and processing. The smart contract software is uploaded on the blockchain network and it is fully autonomous and intelligent [8]. When the contract signed in the agreement by the stakeholders is satisfied the code in the smart contract gets automatically executed.

C. Smart Contracts

The entire execution and the internal operation steps of the blockchain technology is shown in Fig. 4.

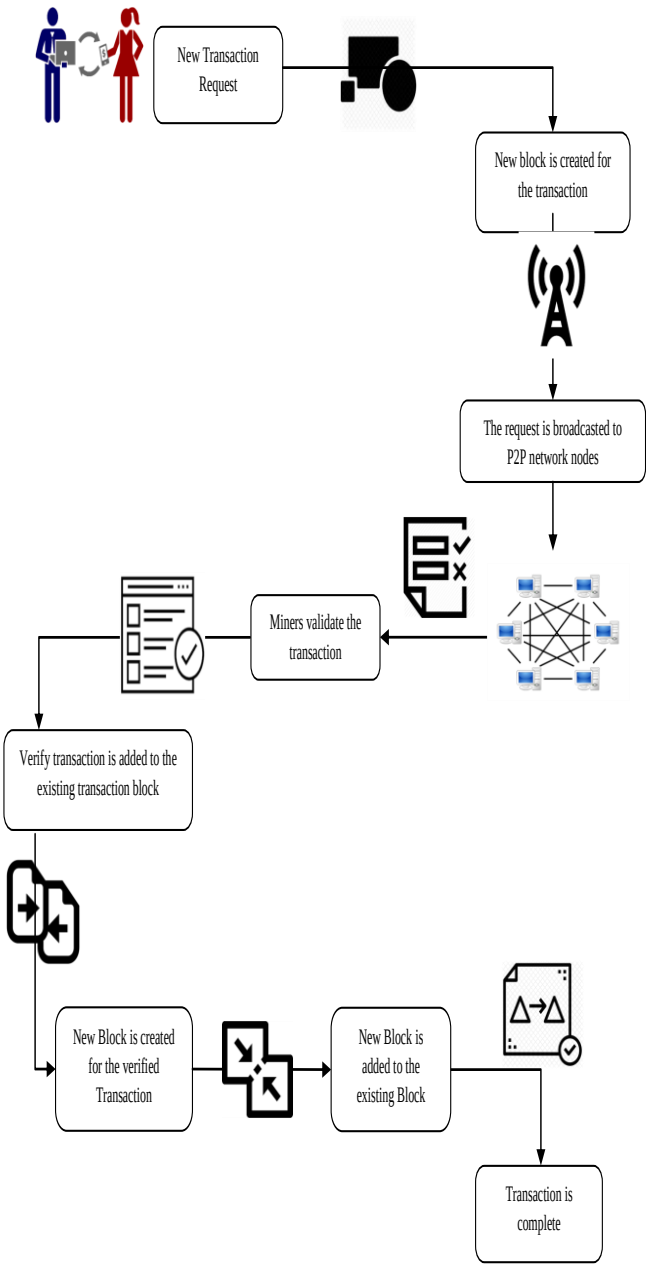

Fig. 5. Blockchain Process

The paper is organized in such a way that Section 2 deals with the preliminaries. Section 3 discuss about the Proposed work. Section 4 discuss about the implementation and the paper is concluded in Section 5.

III. PROPOSED WORK – IOT BLOCKCHAIN BASED DIAMOND INTERNATIONAL TRADE

The proposed structural design for IoT Blockchain based Diamond International Trade is premeditated in this paper. The nodes that are concerned with this IoT Blockchain based Diamond International Trade accept the data information from the predefined real time sensors that are integrated to the things included in the Diamond International Trade. The overall IoT Blockchain based Diamond International Trade architecture is shown below in Fig. 6. The nodes involved in the IoT Blockchain based Diamond International Trade is shown in Fig. 7

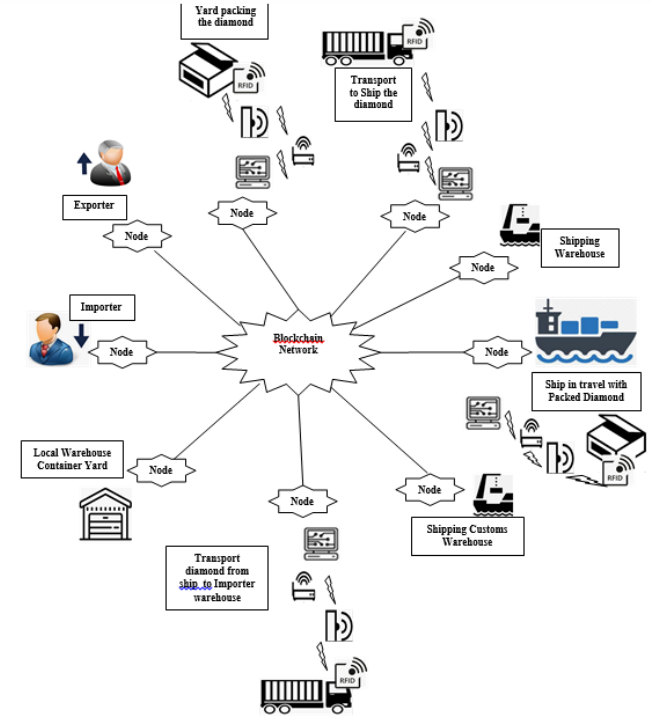

Fig. 6. IoT Blockchain Based Diamond International Trade

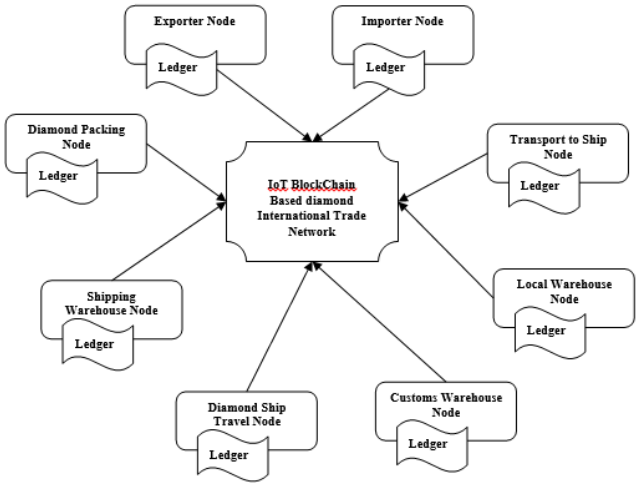

Fig. 7. Nodes in IoT Blockchain Based Diamond International Trade

A. Diamond Packing Node

Each node in the IoT Blockchain based Diamond International Trade network acts as a miner. Every individual node has the private copy of the blockchain with only approved and completed process. The process that are executed in each node consist of the following

- Accessing the sensor data.
- Storing the sensor data.
- Mmonitoring the sensor data.

The process and the actions carried out by the Diamond Packing Node is described in this section. The Operations of the Diamond Packing Node and the use case diagram of Access Diamond Details Transaction in IoT Blockchain Based Diamond International Trade is shown in Fig. 8.

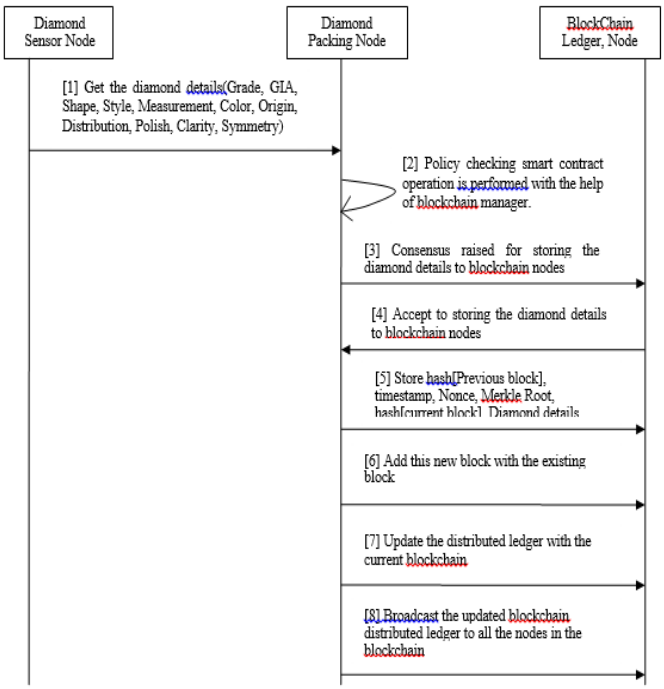

Fig. 8 Use Case Diagram of Access Diamond Details Transaction in IoT Blockchain Based Diamond International Trade

The Algorithm for all the Transactions are shown below,

ALGORITHM 1: Diamond Initial Process

[1] Initialize the packing process
[2] Pack the requested diamond level with respect to the smart contract made by importer.
[3] Pack the diamond with embedding RFID Sensors.
[4] Assign the following attributes
Package id
Address
importer details
Client details
diamond details
Quality details of the diamond
Manufacturer diamond details
other extra attributes.

[5] Receive the diamond package details from the RFID sensors through internet gateways.
[6] Diamond details data is updated in the private cloud storage for the analysis of the data
[7] The processed Diamond data is claimed by the Diamond Packing Node.
[8] End the packing process

The operations that are considered for the Diamond packing node are as follows,

1. Store Diamond Location Transaction
2. Access the Diamond details Transaction
3. Monitor the Diamond Status Transaction

ALGORITHM 2: Store Diamond Location Transaction

[1] Get the location details of the diamond from the Sensor node
[2] Smart contract operation is executed for policy checking in order to store in the blockchain
[3] The location details from other blockchain nodes is updated to perform the consensus
[4] The current location details are updated in the transactions
[5] Update the following details in the blockchain network
hash[Previous block value]
timestamp value
Nonce
Merkle Root value
hash[current block value],
current Location details.
[6] Insert the updated fresh block with the existing block chain.
[7] Revise the updated ledger with the instant blockchain.
[8] Announce and retransmit the restructured ledger to all the nodes in the blockchain
[9] end

ALGORITHM 3: Access Diamond Details Transaction

[1] Get the diamond details of the diamond from the Sensor node
[2] Extract the following details
Diamond Grade Type (A,B,C)
GIA Diamond Report (Unique number assigned to the diamond)
Diamond Shape (square, Rectangle, concave polygons, convex polygons,cyclic polygon, diamond)
Diamond Cutting style (Brilliant, Modified Brilliant, Cushion Modified Brilliant)
Diamond Measurement details (X,Y,Z)
Diamond Carat Weight (carat level)
Diamond Color Grade (color)
Diamond Color Origin (Natural, Artificial)
Diamond Color Distribution (odd ,even)
Diamond clarity (VS1, VS2….etc)
Diamond Polish (Good, Bad)
Diamond Symmetry (Good, Bad)
[3] Smart contract operation is executed for policy checking in order to store in the blockchain
[4] The location details from other blockchain nodes is updated to perform the consensus
[5] The current diamond details are updated in the transactions
[6] Update the following details in the blockchain network
hash[Previous block value]
timestamp value
Nonce
Merkle Root value
hash[current block value],
current Diamond details.
[7] Insert the updated fresh block with the existing block chain.
[8] Revise the updated ledger with the instant blockchain.
[9] Announce and retransmit the restructured ledger to all the nodes in the blockchain
[10] end

ALGORITHM 4: Monitor Diamond status Transaction

[1] Follow and update the continuous change of location information of the diamond from the Sensor node
[2] Retrieve the location information for the priodic time interval based on the smart contract policy.
[3] Smart contract operation is executed for policy checking in order to store in the blockchain
[4] If the predefined time interval is terminated, then retrieve the diamond location information back from the sensor node.
[5] The location details from other blockchain nodes is updated to perform the consensus
[6] The current location details are updated in the transactions
[7] Update the following details in the blockchain network
hash[Previous block value]
timestamp value
Nonce
Merkle Root value
hash[current block value],
current Location details.
[8] Insert the updated fresh block with the existing block chain.
[9] Revise the updated ledger with the instant blockchain.
[10] Announce and retransmit the restructured ledger to all the nodes in the blockchain
[11] end

IV. IMPLEMENTATION AND PERFORMANCE EVALUATION

A. Roof Fall Prediction for Feature Extraction

The Private blockchain network namely ethereum network is used for implementation. The two network are involved in this implementation and they are a follows,

1. Outside owner account node
2. Diamond contract node

The above mentioned nodes are controlled and processed by the Diamond contract node and the monitoring details are shown in “Fig. 9”. The policy further executed when the diamond contract node retrieves anew information from the sensor node involved in the IoT Blockchain based Diamond International Trade blockchain.

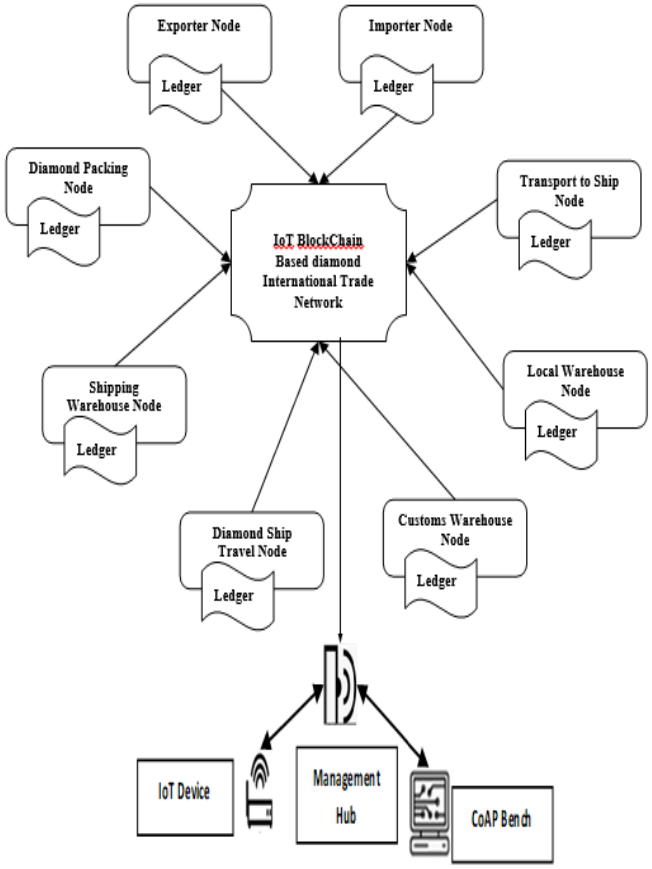

Fig. 9. Implementation Domain in IoT Blockchain Based Satellite Monitoring

The smart devices and the sensor nodes are implemented through LibCoAP Library. Each node process is implemented with the C language using CoAP macros. The predefined LibCoAP macros are updated to repeatedly produce a public/ private key per blockchain node which recognizes the IoT nodes in an unique manner. The benchmark tool namely CoAPBench is used in this paper to test the performance of this designed system. The throughput of the block chain node is estimated that affects the execution delay of the blockchain network and is shown in Fig. 10 and Fig. 11.

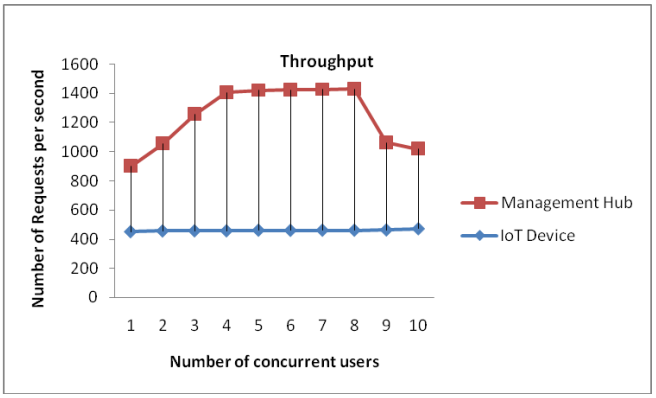

Fig. 10. Throughput of Diamond blockchain node

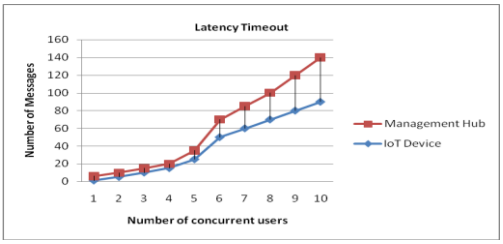

Fig. 11. Timeout Delay of Diamond Packing Node

V. CONCLUSION

In this paper, the preliminary concepts of the blockchain technology are done. In this paper, we have proposed architectural design namely IoT Blockchain Based Diamond International Trade that provides high security and data performance. The Private Blockchain network namely Ethereum blockchain is used for implementation and the results are also discussed. The individual nodes that are involved in the IoT Blockchain Based Diamond International Trade are clearly explained in this paper. The future enhancement is to improve the performance parameters that are involved in the consensus.

REFERENCES

1. Oscar Novo, "Blockchain Meets IoT: An architecture for Scalable Access Management in IoT", IEEE Internet of Things Journal., vol. 5(2), 2018.
2. M. Shyamala Devi, R. Suguna, A. S. Joshi, and R. A. Bagate, "Design of IoT Blockchain Based Smart Agriculture for Enlightening Safety and Security", Emerging Technologies in Computer Engineering: Microservices in Big Data Analytics. ICETCE 2019, Communications in Computer and Information Science, Springer, vol. 985, 2019, pp. 7-19.
3. G. W. Peters, E. Panayi, and A. Chapelle, Trends in crypto-currencies and blockchain technologies: A monetary theory and regulation perspective", SSRN Electronic Journal., 2015
4. L. Lamport, R. Shostak, and M. Pease, "The Byzantine generals problem, ACM Transactions on Programming Languages and Systems", vol. 4(3), 1982, pp. 382-401.
5. Giang-Truong Nguyen, and Kyungbaek Kim, "A Survey about Consensus Algorithms Used in Blockchain", Journal of Information Processing Systems., vol. 14(1), 2018, pp. 101-128.
6. A. Kosba, A. Miller, E. Shi, Z. Wen, Z, and C. Papamanthou, "Hawk: The blockchain model of cryptography and privacy-preserving smart contracts", In: Proceedings of IEEE Symposium on Security and Privacy (SP), 2016, pp. 839–858.
7. Z. Zheng, S. Xie, H. Dai, X. Chen and H. Wang, "Blockchain Challenges and Opportunities: A Survey", International Journal of web and Grid Services., vol. 14(4), 2018.
8. K. Habib, A. Torjusen, and W. Leister, "Security Analysis of a Patient Monitoring System for the Internet of Things in eHealth", In: The Seventh International Conference on eHealth, Telemedicine, and Social Medicine., 2015, pp. 73-78.
9. Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, "An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends", IEEE International Congress on Big Data (BigData Congress), 2017, pp. 557-564.